ENTERPRISE THREAT PROTECTOR

Protezione avanzata dalle minacce nel cloud

Poiché le aziende si servono di DIA (Direct Internet Access), applicazioni SaaS, servizi cloud, mobilità e IoT (Internet of Things), la loro superficie di attacco aumenta notevolmente, portandole a dover affrontare una serie di nuove sfide. Pertanto, diventa sempre più difficile proteggere aziende e utenti da minacce mirate e avanzate, come i malware, il phishing e l'esfiltrazione dei dati. È necessario gestire le complicazioni e le complessità relative ai punti di controllo per la sicurezza, ma anche le lacune nella sicurezza delle soluzioni tradizionali. ETP (Enterprise Threat Protector) è una piattaforma SIG (Secure Internet Gateway) che permette ai team addetti alla sicurezza di offrire a utenti e dispositivi una connessione sicura a Internet ovunque, senza la complessità associata alle altre soluzioni di sicurezza tradizionali. Enterprise Threat Protector è una soluzione controllata da un'intelligence sulle minacce in tempo reale, basata su preziose informazioni globali di Akamai in relazione al traffico Internet e DNS (Domain Name System).

ENTERPRISE THREAT PROTECTOR

Enterprise Threat Protector è una piattaforma SIG basata sull'Akamai Intelligent Edge Platform™ e sul servizio DNS ricorsivo carrier-grade di Akamai, semplice da distribuire e rapida da configurare, che non richiede hardware da installare e mantenere.

Enterprise Threat Protector sfrutta l'Akamai Cloud Security Intelligence in tempo reale e la comprovata piattaforma distribuita a livello globale di Akamai per identificare e bloccare in modo proattivo minacce mirate come malware, ransomware, phishing ed esfiltrazione di dati basata sul DNS. Il portale Akamai consente ai team addetti alla sicurezza di creare, distribuire e applicare, in modo centralizzato e in pochi minuti, sia le policy di sicurezza unificate che le policy di utilizzo (AUP) per tutti i dipendenti, da qualunque punto siano connessi a Internet.

COME FUNZIONA

Enterprise Threat Protector utilizza più livelli di protezione (DNS, URL e analisi dei payload in linea) per offrire una sicurezza ottimale e ridurre la complessità, senza influire sulle performance.

Ispezione DNS: dirigendo semplicemente il traffico DNS ricorsivo esterno verso Enterprise Threat Protector, tutti i domini richiesti vengono confrontati con il punteggio di rischio dei domini in tempo reale di Akamai. Gli utenti vengono bloccati in maniera proattiva per impedire loro l'accesso a domini e a servizi dannosi mentre vengono evase le richieste per domini e servizi sicuri. Dal momento che la convalida avviene prima dell'avvenuta connessione IP, le minacce vengono arrestate preventivamente nella kill chain di sicurezza. Inoltre, il DNS agisce in tutte le porte e in tutti i protocolli, garantendo la protezione dal malware che non utilizza protocolli e porte web standard. È possibile verificare i domini anche per stabilire il tipo di contenuti a cui tenta di accedere un utente ed eventualmente bloccare i domini se i contenuti rappresentano una violazione dell'AUP aziendale.

Ispezione URL: i domini vengono considerati rischiosi in base all'intelligence Akamai relativa alle minacce automaticamente inoltrate a un proxy basato su cloud sull'Akamai Intelligent Edge Platform. L'URL richiesto viene verificato rispetto all'intelligence delle minacce degli URL di Akamai e gli URL dannosi vengono automaticamente bloccati. Il proxy ispeziona sia gli URL HTTP che HTTPS.

Analisi dei payload in linea: i payload HTTP e HTTPS di domini rischiosi vengono poi sottoposti a scansione in tempo reale tramite più motori avanzati di rilevamento dei malware. Questi motori utilizzano varie tecniche (come l'apprendimento con firma, senza firma e automatico) che offrono una protezione zero-day completa contro file potenzialmente dannosi, come file eseguibili e di documento, nonché altri malware incorporati direttamente nella pagina web richiesta, come codice JavaScript dannoso e nascosto.

Enterprise Threat Protector si integra senza problemi con altri prodotti di sicurezza e strumenti per la creazione di rapporti, tra cui firewall e SIEM e feed di intelligence delle minacce esterne, per consentirvi di ottimizzare gli investimenti in tutti i livelli dello stack di sicurezza dell'azienda.

Inoltre, l'implementazione del connettore Enterprise Client Connector "leggero" su laptop gestiti consente alle aziende di aggiungere rapidamente un ulteriore livello di sicurezza proattiva quando i laptop vengono utilizzati al di fuori della rete.

VANTAGGI PER LE AZIENDE

- **Ottimizzazione delle difese di sicurezza** bloccando in modo proattivo le richieste indirizzate a siti che diffondono malware e ransomware, server CnC (Command and Control) relativi a malware e domini di phishing ed esfiltrazione dei dati DNS, nonché URL che si basano su un'intelligence delle minacce esclusiva e aggiornata.
- **Blocco dei payload dannosi per una migliore protezione zero-day** sottoponendo a scansione i file e i contenuti web richiesti in tempo reale, al fine di arrestare le minacce prima che possano raggiungere e compromettere i dispositivi endpoint.
- **Miglioramento delle performance di DIA** con un proxy del traffico sospetto per l'ispezione dell'URL e l'analisi dei payload.
- **Aggiunta di protezione immediata senza hardware o complessità associate** con una soluzione totalmente basata sul cloud che può essere configurata e distribuita globalmente in pochi minuti (senza interruzioni per gli utenti) e scalata rapidamente.
- **Riduzione dei rischi e maggiore sicurezza per i laptop al di fuori della rete senza utilizzo di VPN** , grazie al connettore Enterprise Client Connector "leggero" che rafforza le misure di sicurezza e le AUP.
- **Minimizzazione dei tempi e della complessità di gestione della sicurezza** riducendo gli avvisi di sicurezza di falsi positivi, aumentando quelli provenienti da altri prodotti di sicurezza e gestendo le policy e gli aggiornamenti di sicurezza da qualunque luogo e in pochi secondi, al fine di proteggere tutte le sedi.
- **Applicazione rapida e uniforme della conformità e delle policy di utilizzo** bloccando l'accesso a categorie di contenuti e domini inappropriati o discutibili.
- **Incremento della resilienza e dell'affidabilità del DNS** con l'Akamai Intelligent Edge Platform.

ENTERPRISE THREAT PROTECTOR

CSI (CLOUD SECURITY INTELLIGENCE) DI AKAMAI

Enterprise Threat Protector si basa su Cloud Security Intelligence di Akamai, una soluzione che offre intelligence in tempo reale sulle minacce e sui rischi che tali minacce comportano per le aziende.

L'intelligence Akamai relativa alle minacce è progettata per fornire protezione dalle minacce attuali e pertinenti, che potrebbero influenzare negativamente l'azienda, ma anche per ridurre al minimo il numero di avvisi di falsi positivi da far approfondire ai propri team addetti alla sicurezza.

Questa intelligence si basa sui dati raccolti ogni giorno dall'Akamai Intelligent Edge Platform, che gestisce fino al 30% del traffico web globale e distribuisce ogni giorno fino a 2,2 trilioni di query DNS. L'intelligence di Akamai è migliore grazie a un ampio numero di feed delle minacce esterne e i set di dati, così combinati, vengono continuamente analizzati e trattati con avanzate tecniche di analisi comportamentale, funzioni di apprendimento automatico e algoritmi proprietari. A mano a mano che vengono identificate nuove minacce, queste vengono immediatamente aggiunte al servizio Enterprise Threat Protector, garantendo protezione in tempo reale.

AKAMAI INTELLIGENT EDGE PLATFORM

Il servizio Enterprise Threat Protector si basa sull'Akamai Intelligent Edge Platform carrier-grade, una piattaforma sicura, affidabile e veloce. Distribuita a livello globale, offre una disponibilità totale coperta da SLA (accordo sul livello di servizio) e un'affidabilità ottimale per il servizio DNS ricorsivo dell'azienda.

PORTALE DI GESTIONE BASATO SUL CLOUD

Tutte le attività di configurazione e gestione continua di Enterprise Threat Protector vengono eseguite tramite il portale Luna basato su cloud di Akamai, rendendo possibile la gestione in qualsiasi luogo e momento.

La gestione delle policy è semplice e veloce e le modifiche possono essere inoltrate a livello globale in pochi minuti per garantire la protezione di tutte le sedi e di tutti gli utenti. Gli avvisi in tempo reale tramite e-mail e i rapporti programmati possono essere configurati per avvisare i team addetti alla sicurezza degli eventi critici relativi alle policy, affinché sia possibile intervenire immediatamente per identificare e risolvere le potenziali minacce. Un dashboard in tempo reale fornisce una panoramica del traffico, delle minacce e degli eventi correlati alle policy di utilizzo. Le informazioni dettagliate sulle attività possono essere visualizzate tramite un'analisi approfondita dei singoli elementi del dashboard. Queste informazioni dettagliate costituiscono un'importante risorsa per l'analisi e la correzione degli incidenti relativi alla sicurezza.

Tutte le funzionalità del portale sono accessibili tramite API e i registri di dati possono essere esportati in un SIEM, consentendo così a Enterprise Threat Protector di integrarsi in modo semplice ed efficace con gli altri strumenti per la creazione di rapporti e con altre soluzioni di sicurezza.

FUNZIONALITÀ PRINCIPALI

- **Minacce categorizzate da Akamai:** l'intelligence delle minacce costantemente aggiornata in base alla visibilità di Akamai sul 15-30% del traffico web giornaliero si unisce a 2,2 trilioni di richieste DNS al giorno indirizzate al cloud DNS ricorsivo di Akamai.
- **Minacce categorizzate dal cliente:** i team addetti alla sicurezza sono in grado di integrare rapidamente i feed di intelligence delle minacce esistenti, ottimizzando il valore degli investimenti attuali in ambito di sicurezza.
- **Analisi in tempo reale dei payload in linea:** tre motori di rilevamento malware avanzati identificano e bloccano le minacce avanzate più complesse, migliorando la protezione zero-day.
- **Policy di utilizzo:** applicazione di policy di utilizzo aziendali e garanzia del rispetto della conformità alla limitazione delle categorie di contenuti accessibili.
- **Analisi e creazione di rapporti:** i dashboard offrono informazioni in tempo reale su tutto il traffico web aziendale in uscita, nonché sugli eventi relativi alle minacce e alle policy di utilizzo.
- **Informazioni sulla sicurezza:** rapida comprensione del motivo per cui Akamai abbia aggiunto un dominio o un URL ai propri elenchi di minacce per l'intelligence.
- **Log:** i log del traffico vengono conservati per 30 giorni e possono essere facilmente esportati in un file CSV o integrati in un SIEM per un'analisi più approfondita.
- **DNSSEC:** in tutte le richieste DNS inviate a Enterprise Threat Protector è abilitato DNSSEC.

L'ECOSISTEMA AKAMAI

L'Akamai Intelligent Edge Platform permea ogni ambito, dalle aziende al cloud, permettendovi di lavorare con rapidità, efficacia e sicurezza. Le nostre soluzioni complete vengono gestite tramite il portale unificato e personalizzabile Luna Control Center, che garantisce visibilità e controllo, e sono supportate dagli esperti del team Professional Services, che aiuta i clienti a essere subito operativi proponendo loro soluzioni sempre nuove, in linea con l'evoluzione delle strategie aziendali.

Per maggiori informazioni su Enterprise Threat Protector e per accedere a una prova gratuita, visitate il sito akamai.com/etp.

Akamai

ENTERPRISE THREAT PROTECTOR

SICUREZZA	Guest Wi-Fi	Intelligence	Advanced Threat
Blocco di malware, ransomware e domini di delivery di phishing		X	X
Blocco di richieste CnC (Command and Control) relative ai malware		X	X
Identificazione dell'esfiltrazione dei dati basata sul DNS		X	X
Domini per proxy dannosi per l'ispezione degli URL HTTP e HTTPS richiesti		X	X
Analisi in linea in tempo reale di payload HTTP e HTTPS tramite l'analisi di più malware in linea e motori di rilevamento			X
Analisi in linea in tempo reale dei file scaricati dai siti di condivisione file			X
Creazione di un elenco personalizzato di domini per l'ispezione di URL HTTP e HTTPS		X	X
Creazione di un elenco personalizzato di domini per l'analisi dei payload in linea			X
Analisi lookback dei registri del traffico di clienti per identificare e avvisare in caso vengano rilevate nuove minacce		X	X
Creazione di elenchi personalizzati di tipo Consenti/Rifiuta		X	X
Integrazione di altri feed di intelligence delle minacce esterne		X	X
Pagine di errore personalizzabili	X	X	X
Interrogazione del database di minacce di Akamai per accedere all'intelligence sui domini e sugli URL dannosi		X	X
Applicazione della sicurezza per laptop al di fuori della rete (Windows e macOS)		X	X
POLICY DI UTILIZZO (AUP)	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Monitoraggio o blocco delle violazioni AUP per utenti all'interno e all'esterno della rete	X[1]	X	X
Applicazione della SafeSearch su Google, Bing e YouTube	X	X	X
GENERAZIONE DI RAPPORTI, MONITORAGGIO E GESTIONE	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Visualizzazione a livello aziendale di tutte le attività con dashboard personalizzabili	X[2]	X	X
Analisi dettagliata di tutte le minacce ed eventi AUP	X[2]	X	X
Log completi e visibilità per tutte le richieste di traffico pubblicato, nonché per gli eventi di minacce e AUP	X[2]	X	X
Delivery di tutti i registri; i registri vengono conservati per 30 giorni ed è possibile esportarli tramite un'API	X[2]	X	X
Configurazione, elenchi di sicurezza personalizzati ed eventi disponibili tramite un'API aperta	X[2]	X	X
Integrazione con altri sistemi di sicurezza, come SIEM, tramite un'API aperta	X	X	X
Sicurezza in tempo reale basata su e-mail e avvisi AUP	X[2]	X	X
Pianificazione di rapporti giornalieri o settimanali ricevuti tramite e-mail	X	X	X
Amministrazione delegata	X	X	X
AKAMAI INTELLIGENT EDGE PLATFORM™	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
VIP IPv4 e IPv6 dedicati per ogni cliente, per DNS ricorsivo	X	X	X
SLA per il 100% di disponibilità	X	X	X
Routing DNS Anycast per performance ottimali	X	X	X
DNSSEC applicato per una maggiore sicurezza	X	X	X
CONNETTORI AZIENDALI	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Enterprise Client Connector per proteggere i laptop al di fuori della rete (Windows e OSX) e per comunicare il nome del computer in caso di eventi all'interno e all'esterno della rete		X	X
Aggiornamento automatico di Enterprise Client Connector		X	X
Enterprise Security Connector per l'identificazione degli indirizzi IP e dei nomi dei computer dei dispositivi endpoint		X	X

1. ETP Guest Wi-Fi non comprende l'applicazione dell'AUP al di fuori della rete.
2. ETP Guest Wi-Fi non comprende alcun controllo di sicurezza, pertanto gli avvisi, l'analisi, i dashboard e i registri includono solo eventi e attività AUP.